AMENDED IN ASSEMBLY AUGUST 15, 2005

AMENDED IN ASSEMBLY JULY 7, 2005

AMENDED IN ASSEMBLY JUNE 23, 2005

AMENDED IN ASSEMBLY JUNE 15, 2005

AMENDED IN SENATE MAY 11, 2005

AMENDED IN SENATE MAY 4, 2005

AMENDED IN SENATE MARCH 31, 2005

SENATE BILL No. 682

Introduced by Senator Simitian
(Coauthor: Assembly Member Evans)

February 22, 2005

An act to add Article 4 (commencing with Section 1798.9) to Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, relating to privacy.

LEGISLATIVE COUNSEL'S DIGEST

SB 682, as amended, Simitian. Identity Information Protection Act of 2005.

Existing law, the Information Practices Act of 1977, regulates the collection and disclosure of personal information regarding individuals by state agencies, except as specified. The intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the act is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains.

This bill would enact the Identity Information Protection Act of 2005. The act would require identification documents, except as specified, that are created, mandated, purchased, or issued by various public entities~~, and~~ that ~~contain a contactless integrated circuit or other device that uses~~ *use* radio waves to broadcast personal information*,* or to enable personal information to be read remotely, to meet specified requirements. The bill would provide that a person or entity that ~~knowingly or willfully~~ *intentionally* remotely reads or attempts to remotely read a person's identification document using radio waves without his or her knowledge shall be punished by imprisonment in a county jail for up to one year, a fine of not more than $5,000, or both that fine and imprisonment.

In addition, because the intentional disclosure of medical, psychiatric, or psychological information in violation of the disclosure provisions of the Information Practices Act of 1977, which would include this act, is punishable as a misdemeanor if the wrongful disclosure results in economic loss or personal injury to the individual to whom the information pertains, and because remotely reading or attempting to remotely read a person's identification document without his or her knowledge would be punishable as a misdemeanor, this bill would create a new crime, thereby imposing a state-mandated local program.

The California Constitution requires the state to reimburse local agencies and school districts for certain costs mandated by the state. Statutory provisions establish procedures for making that reimbursement.

This bill would provide that no reimbursement is required by this act for a specified reason.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: yes.

The people of the State of California do enact as follows:

SECTION 1. This act shall be known and may be cited as the Identity Information Protection Act of 2005.

SEC. 2. The Legislature hereby finds and declares all of the following:

(a) The right to privacy is a personal and fundamental right protected by Section 1 of Article I of the California Constitution and by the United States Constitution. All individuals have a right of privacy in information pertaining to them.

(b) Easy access to the information found on drivers' licenses and other similar identification documents facilitates the crime of identity theft, a crime that is a major concern in California. More than 43,000 Californians reported being victims of this crime in 2004.

(c) This state has previously recognized the importance of protecting the confidentiality and privacy of an individual's personal information contained in identification documents such as drivers' licenses.

(d) ~~The inclusion in identification documents of contactless integrated circuits or other devices~~ *Identification documents* that use radio waves to broadcast data or to enable data to be scanned secretly and remotely will greatly magnify the potential risk to individual privacy, safety, and financial security that can occur from unauthorized interception and use of personal information. ~~The inclusion of those devices~~ *These identification documents* will also make it possible for any person or entity with access to a reader to engage in the secret tracking of Californians on an unprecedented scale.

SEC. 3. Article 4 (commencing with Section 1798.9) is added to Chapter 1 of Title 1.8 of Part 4 of Division 3 of the Civil Code, to read:

Article 4. Identity Documents

1798.9. For purposes of this article, the following definitions shall apply:

(a) "Authentication" means the process of applying a specific mathematical algorithm to data or identification documents, or both, so as to accomplish either of the following:

(1) Prove or establish that the data and the identification document containing the data~~, including any contactless integrated circuit in the identification document,~~ were issued by the responsible issuing state or local governmental body.

(2) Ensure that a reader, as defined in subdivision ~~(h)~~*(l)*, is permitted under California law to access such data or identification document.

(b) "Authorized reader" means a reader, as defined in subdivision ~~(h)~~*(l)*, that, with respect to a particular identification document, (1) is permitted under California law to remotely read the personal information broadcast or transmitted by that identification document, (2) is being used for a lawful purpose, and (3) is fully in accord with the requirements of subdivision (a) of Section 1798.10.

~~(c) "Contactless integrated circuit" means a data carrying unit, such as an integrated circuit or computer chip, that can be read remotely.~~

~~(d)~~

(c) "Contactless identification document system" means a group of identification documents issued and operated under a single authority that use radio waves to transmit personal information remotely to readers intended to read that information. In a contactless identification document system, every reader must be able to read every identification document in the system.

(d) "Cryptographic protocol" means a sequence of interactions between two parties to ensure that only authorized parties can communicate with one another.

(e) "Encryption" means the process of applying a specific mathematical algorithm to data so as to protect the confidentiality of that data by rendering that data unintelligible to an unauthorized party.

~~(e)~~

(f) "Identification document" means any document containing personal information that an individual uses alone or in conjunction with any other information to establish his or her identity. Identification documents specifically include, but are not limited to, the following:

(1) Driver's licenses or identification cards.

(2) Identification cards for employees or contractors.

(3) Identification cards issued by educational institutions.

(4) Health insurance or benefit cards.

(5) Benefit cards issued in conjunction with any government-supported aid program.

(6) Licenses, certificates, registration, or other means to engage in a business or profession regulated by the Business and Professions Code.

(7) Library cards issued by any public library.

~~(f)~~

(g) "Key" means a string of bits of information used as part of a cryptographic algorithm used in encryption.

(h) "Key establishment" means a protocol by which two parties jointly generate a key for use in a subsequent cryptographic protocol.

(i) "Mutual authentication" means the use of authentication, as defined in subdivision (a), to ensure that authorized readers, as defined in subdivision (b), can reliably detect unauthorized identification documents, and that authorized identification documents can be read only by those authorized readers.

~~(g)~~

(j) "Personal information" includes any of the following: an individual's name, address, telephone number, e-mail address, date of birth, religion, ethnicity, nationality, photograph, fingerprint or other biometric identification, social security number, or any other unique personal identifier or number.

~~(h)~~

(k) "Public-key" means a form of cryptography in which the key is split into two parts, a public key, which is known to all, and a secret key, which is known to only one party.

(l) "Reader" means a scanning device that is capable of using radio waves to communicate with~~ a contactless integrated circuit or other device using radio waves~~ *an identification document* and read the personal information broadcast or transmitted by that ~~integrated circuit or other device~~ *identification document*.

~~(i)~~

(m) "Remotely" means that no physical contact between the ~~integrated circuit or device~~ *identification document* and a reader is necessary in order to transmit data.

~~(j)~~

(n) "Session" is a sequence of interactions between the identification document and the reader that represents one logical reading of the identification document by the reader and begins when either the reader or identification document initiates communication with the other and ends when either the reader or identification document becomes out of range or explicitly sends a message closing the session.

(o) "Session key" means a key used only for a single session between two parties.

(p) “Shared secret” means a key shared between two parties and no others.

(q) “Shield devices” mean physical or technological protections available to stop the broadcast or transmission of personal information programmed on or into ~~a contactless integrated circuit or other devices~~ *an identification document* using radio waves.

~~(k)~~

(r) “Single episode of care” means an inpatient hospital stay through discharge or specific course of therapy or treatment for outpatient care.

(s) “Unique identifier number” means a ~~random~~ *randomly assigned* string of numbers that is encoded onto the ~~contactless integrated circuit or other device~~ *identification document*.

1798.10. (a) Except as provided in subdivisions (b) and (c), all identification documents created, mandated, purchased, or issued by a state, county, or municipal government, or subdivision or agency thereof that ~~contain a contactless integrated circuit or other device that uses radio waves to broadcast~~ *use radio waves to transmit* personal information or to enable personal information to be read remotely shall meet these requirements:

(1) The identification document shall not ~~contain, transmit,~~ *transmit* or enable the remote reading of any personal information other than a unique personal identifier number ~~in or from its contactless integrated circuit or other device that uses~~ *using* radio waves.

(2) *(A)* The identification document shall implement ~~strong encryption to protect against the unauthorized reading of transmitted information. The confidentiality provided by that encryption shall at all times be at least as strong as RSA encryption using a key length of 1024 bit as understood on the effective date of this article. In the event that this standard is cracked and hence no longer capable of protecting against the unauthorized reading of transmitted information, the identification document shall implement a stronger encryption standard that will ensure protection against the unauthorized reading of transmitted information.~~

~~(3) The identification document shall implement mutual authentication to protect against the unauthorized transmission of~~

~~information from the identification document to unauthorized readers. The protection provided by that mutual authentication shall at all times and at a minimum incorporate the highest standards of active mutual authentication contained in the document issued by the International Organization for Standards known as the Common Criteria ISO 15408 or its equivalent as subsequently updated. The identification document shall in no case incorporate a lower standard for active mutual authentication than the highest standard articulated by Common Criteria ISO 15408 at the time of the effective date of this article.~~ *mutual authentication in order to prevent the transmission of information between identification documents and unauthorized readers. The mutual authentication standard shall at all times be at least as strong as any non-escrowed card authentication standard for algorithm and key parameters approved and specified by National Institute of Standards and Technology Special Publication 800-78 (NIST SP 800-78) for use after December 31, 2010, or its successor if NIST SP 800-78 is amended or replaced. Proprietary encryption shall not be used. In the event that the card authentication standard used in an identification document is found to be no longer capable of protecting against the transmission of information between identification documents and unauthorized readers, a stronger card authentication standard that will ensure protection shall be implemented. Either a shared-secret or public-key cryptographic protocol may be used for mutual authentication.*

(B) The identification document shall also implement key establishment, so that if mutual authentication is successful, the identification document and the authorized reader shall derive a session key at least 16 bytes long for use with the secure-messaging encryption required under paragraph (3) of subdivision (a).

(3) The identification document shall implement strong encryption to protect against the unauthorized reading of information transmitted between the identification document and reader after mutual authentication as described in paragraph (2) of subdivision (a) is concluded. This encryption shall not use proprietary encryption, and shall at all times be at least as strong as, or use, an approved non-escrowed encryption standard for algorithm and key parameters specified in Federal

Information Processing Standards Publication 140-2 Annex A (FIPS Pub. 140-2 Annex A) or its successor if FIPS Pub. 140-2 Annex A is amended or replaced. In the event that the encryption standard used in an identification document is found to be no longer capable of protecting against the unauthorized reading of transmitted information, a stronger encryption standard that will ensure protection against the unauthorized reading of transmitted information shall be implemented.

(4) In order to ensure that the holder of the identification document affirmatively consents to each reading of the identification document, each identification document shall implement at least one of the following privacy safeguards:

(A) An access control protocol requiring the optical or other nonradio frequency reading of information from the identification document prior to each transmission or broadcast of data using radio waves, without which the identification document will not transmit or broadcast personal information using radio waves.

(B) A shield device that, when used to protect the identification document, can prevent any communication of data using radio waves between the ~~contactless integrated circuit~~ *identification document* and any reader under any circumstances.

(C) A ~~contactless integrated circuit or other device~~ *data-carrying device, such as an integrated circuit or computer chip,* that is normally not remotely readable, accessible, or otherwise operational under any circumstances, and only remotely readable, accessible, or operational while being temporarily switched on or otherwise intentionally activated by a person in physical possession of the identification document. The device shall only be remotely readable while the person intentionally uses the switch intending that the identification document be read.

(5) The issuing entity of an identification document shall communicate in writing to the person to whom the document is issued *at or before the time the document is issued*, all of the following:

(A) That the identification document ~~contains a contactless integrated circuit or device that~~ can ~~broadcast~~ *transmit* a unique personal identifier number or enable that number to be read remotely without his or her knowledge.

(B) That countermeasures, such as shield devices, may be used to help the person control the risk that his or her unique personal identifier number will be broadcast or read remotely without his or her knowledge.

(C) The location of all readers used or intended to be used by the issuing authority ~~or by any other entity known to that authority~~ to read the unique personal identifier number on the identification document. *Alternatively, the issuing authority may satisfy this reader-location notice requirement by doing both of the following:*

(i) Providing each document holder with a general description of the locations or types of locations where readers are used, such as all agency building entrances and exits.

(ii) Posting or displaying a clear and conspicuous sign, placard, poster, or other similar written notice at each reader's actual location stating that the issuing authority has placed an identification document reader at that location, the reader is being used to read identification documents remotely using radio waves, and the commonly understood name of each document.

(D) Any ~~information~~ *information, such as time and location,* that is being collected ~~at the time the contactless integrated circuit or other device is read or that is being~~ *or* stored regarding the individual in a database *at the time the identification document is being read*.

~~(E) Additional annual notice shall be communicated in writing of any new shield devices in existence or~~

(6) The issuing authority of any identification document shall provide annual notice to the person to whom the document is issued of any changes in the location of readers or the information collected or stored in the database *if changes have occurred*.

(b) Subdivision (a) shall not apply to:

(1) An identification document that is part of a contactless ~~integrated~~ *identification document* system used by a state, county, or municipal government, or subdivision or agency thereof that is operational and in use prior to January 1, 2006, if all of the following apply:

(A) The ~~system~~ *identification document* is not used for any purpose other than the purpose or purposes of the system on the effective date of this article.

(B) The~~ amount, type, or types of information stored, broadcast, or transmitted by the contactless integrated circuit is the same as, or less or fewer than,~~ *identification document does not transmit using radio waves a greater amount, type, or types of information than the identification document in use* on the effective date of this article.

~~(C) The contactless integrated circuit is being issued to the same group or groups as, or fewer or smaller groups of people than, were issued the contactless integrated circuit on the~~

(C) The identification document is not issued to any group or category of people that was not issued the identification document on the effective date of this article.

(2) An identification document issued to a person who is incarcerated in the state prison or a county jail, detained in a juvenile facility operated by the Division of Juvenile Facilities in the Department of Corrections and Rehabilitation, or housed in a mental health facility, pursuant to a court order after having been charged with a crime, or to a person pursuant to court-ordered electronic monitoring.

(3) An identification document issued to a person employed by a state prison, county jail, or juvenile facility operated by the Division of Juvenile Facilities in the Department of Corrections and Rehabilitation if the document is not removed from the facility and the requirements of paragraph (5) of subdivision (a) apply.

(4) An identification document issued to a firefighter or emergency medical technician if the document is used only while the firefighter or emergency medical technician is on active duty and the requirements of paragraph (5) of subdivision (a) apply.

(5) An identification document issued to a patient who is in the care of a government-operated hospital, ambulatory surgery center, or oncology or dialysis clinic if~~ the document is (A) valid~~ *all of the following requirements are met:*

(A) The identification document is valid for only a single episode of~~ care, (B) removed from the patient at the time the patient is discharged, and (C) contains no personal information other than a unique identifier number, and a patient returning for a new episode of care is assigned a new unique identifier number.~~ *care.*

(B) The identification document may be removed and reattached when used on a nonemergency outpatient.

(C) The identification document complies with paragraph (1) of subdivision (a).

(D) The patient returning for a new episode of care is assigned a new unique identifier number.

(E) The patient is notified, in writing, that the identification document transmits personal information using radio waves.

(F) The patient is not compelled or encouraged to wear, or keep on his or her person, the identification document beyond the facility property.

(6) An identification document issued to a patient by emergency medical services for triage or medical care during a disaster and immediate hospitalization or immediate outpatient care directly related to a disaster, as defined by the local Emergency Medical Services agency organized under Section 1797.200 of the Health and Safety Code.

(7) An identification document issued to a person for the limited purpose of collecting funds for the use of a toll bridge, such as the FasTrak system, if the requirements of paragraphs (1)~~, (4),~~ and (5) of subdivision (a) are met.

(8) An identification document that is issued to a person for the limited purpose of facilitating secured access by the identification document holder to a secured public building or parking area, if the requirements of paragraphs (1)~~, (4),~~ and (5) of subdivision (a) are met.

(9) A license, certificate, registration, or other authority for engaging in a business or profession regulated under the Business and Professions Code, if the requirements of paragraphs (1), (4), and (5) of subdivision (a) are met.

(10) An identification document for which the Legislature determines that the standards of subdivision (a) of Section 1798.10 do not apply because of the existence of a compelling state interest and that there is no means less intrusive to the individual's privacy and security to achieve the compelling state interest.

(c) *(1)* Except for identification documents listed in subdivision (b), the following identification documents created, mandated, purchased, or issued by a state, county, or municipal government, or subdivision or agency thereof, shall not ~~contain a~~

~~contactless integrated circuit or other device that uses radio waves to broadcast~~ *use radio waves to transmit* personal information or to enable personal information to be read remotely:

~~(1)~~

(A) Drivers' licenses or identification cards issued pursuant to Section 13000 of the Vehicle Code.

~~(2)~~

(B) Identification cards issued to students in K-12 schools.

~~(3)~~

(C) Health insurance, health benefit, and benefit cards issued in conjunction with any government-supported aid program.

~~(4)~~

(D) Library cards issued by any public library.

~~This~~

(2) This subdivision shall become inoperative on January 1, 2009, unless a later enacted statute deletes or extends that date.

1798.11. Except as provided in subdivision (d), a state, county, or municipal government, or subdivision or agency thereof that creates, mandates, purchases, or issues an identification document in compliance with subdivision (a) of Section 1798.10 or a third party with whom the governmental agency has a bona fide business relationship:

(a) Shall not, under any circumstances, disclose the keys required by paragraph (2) of subdivision (a) of Section 1798.10, either publicly or to any nongovernmental entity or other third party, including, but not limited to, contractors, officers, and employees of other government agencies.

(b) Shall take all reasonable measures to keep the keys required by paragraph (2) of subdivision (a) of Section 1798.10 unavailable to any third party.

(c) Shall not, under any circumstances, act in any way to allow a third party to read the personal information broadcast or transmitted remotely by the identification document using radio waves.

(d) A state, county, or municipal government, or a political subdivision or agency thereof, and a single third party with whom the governmental agency has entered into a contract, either for operation, monitoring, or technical assistance, may disclose the keys to each other and allow each other to read the

personal information broadcast or transmitted remotely by the identification document using radio waves. A single third party with whom the governmental entity has entered into a contract shall agree to the following conditions:

(1) The third party shall adopt procedures restricting access to the keys, and these procedures shall be designed to secure the keys from tampering and unauthorized access. These procedures shall include administrative, technical, and physical safeguards to protect against any reasonably anticipated threats or hazards to the privacy of the information, and unauthorized uses or disclosures of the information.

(2) The third party shall not transmit the keys to any other person or entity.

(3) Any person or entity who receives a disclosure pursuant to this exception is subject to the prohibition of subdivision (a). All information received pursuant to this exception shall be destroyed when the purpose of the disclosure is completed.

(4) Any person may bring a civil action against a governmental entity whenever the governmental entity, third party entity with whom the governmental entity has entered into a contract, or third party with whom the governmental entity has a bona fide business relationship fails to comply with the provisions of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on a person. For purposes of this paragraph, "adverse effect" includes, but is not limited to any time a third party that enters into a bona fide business relationship pursuant to this subdivision, subsequently discloses that information to another person, regardless of whether economic harm occurred.

1798.12. A state, county, or municipal government, or a political subdivision or agency thereof, that uses radio waves to broadcast personal information or to enable personal information to be read remotely pursuant to subdivision (a) of Section 1798.10 or the single third party entity with whom the governmental entity has entered into a contract or third party with whom the governmental entity has a bona fide business relationship shall not disclose any personal information, information regarding the location of a person derived from the use of the radio waves, or the keys required by paragraph (2) of *subdivision (a) of Section 1798.10, unless the disclosure is required pursuant to a search warrant.*

~~1798.12.~~

1798.13. A person or entity that ~~knowingly or willfully~~ *intentionally* remotely reads or attempts to remotely read a person's identification document *issued pursuant to Section 1798.10* using radio waves, without the knowledge of that person shall be punished by imprisonment in a county jail for up to one year, a fine of not more than five thousand dollars ($5,000), or both that fine and imprisonment.

SEC. 4. No reimbursement is required by this act pursuant to Section 6 of Article XIII B of the California Constitution because the only costs that may be incurred by a local agency or school district will be incurred because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction, within the meaning of Section 17556 of the Government Code, or changes the definition of a crime within the meaning of Section 6 of Article XIII B of the California Constitution.

O